International Journal of Law and Information Technology, 2021, 29, 57–75
doi: 10.1093/ijlit/eaaa022
Advance Access Publication Date: 25 January 2021
Article

OXFORD

The territorial effect of the right to be forgotten after *Google v CNIL*

P.T.J. (PIETER) WOLTERS*

ABSTRACT

In *Google v CNIL*, the Court of Justice has ruled that the right to be forgotten does not compel a search engine to delist a website in its non-European versions. At first sight, *Google v CNIL* therefore seriously undermines the effectiveness of the right to be forgotten. However, further analysis reveals that this conclusion is premature. First, the effectiveness depends on the requirements on the measures to prevent or at least seriously discourage users in the European Union from accessing the delisted website through a search with the name of the data subject as a search criterion. Next, the effectiveness of the right to be forgotten depends on the requirements of national standards of protection of fundamental rights. The GDPR does not prohibit member states from ordering search engines to also delist a website in non-European versions.

KEYWORDS: GDPR, Right to be forgotten, fundamental rights

INTRODUCTION

The World Wide Web has a global character.[1] For example, an 'American' website is not only available in the USA, but also in the rest of the world. Its content is not necessarily restricted to American issues. For example, it could also contain information about the citizens of the European Union. This global character raises questions regarding the territorial effect of data protection law and other legal rules.[2]

Google Spain shows that the 'right to be forgotten' in the General Data Protection Regulation (GDPR) can be used to compel a search engine to remove a website

* P.T.J. (Pieter) Wolters is Associate Professor in civil law at the Radboud University Nijmegen, The Netherlands. He is a member of the Radboud Business Law Institute, and of the Interdisciplinary Hub for Security, Privacy and Data Governance (iHub)

1 As will be discussed in the sections 'The Effectiveness of Geo-Blocking' and 'Additional Measures', 'Geo-blocking' and censorship can cause fragmentation by blocking access to certain websites based on the location of the user. See eg Jakub Dalek and others, 'A Method for Identifying and Confirming the Use of URL Filtering Products for Censorship' in *IMC '13 Proceedings of the 2013 conference on Internet measurement conference* (ACM 2013), 23; Allison McDonald and others, '403 Forbidden: A Global View of CDN Geoblocking' in *IMC'18. Proceedings of the Internet Measurement Conference* (ACM 2018), 218.

2 eg Paul de Hert and Michal Czerniawski, 'Expanding the European Data Protection Scope Beyond Territory: Article 3 of the General Data Protection Regulation in its Wider Context' (2016) 6 IDPL 230, 230.

© The Author(s) (2021). Published by Oxford University Press. All rights reserved.
For permissions, please email: journals.permissions@oup.com.

Downloaded from https://academic.oup.com/ijlit/article/29/1/57/6118444 by guest on 16 April 2021

from the list of search results.[3] The effectiveness of this right depends in part on its 'territorial effect' or 'scope'.[4] The right is less effective if the delisted website can still be found by using a non-European search engine. This is particularly important because search engines like Google operate a separate version for each country.[5]

In *Google v CNIL*,[6] the (French) Conseil d'État raised the question whether the European right to be forgotten can compel a search engine to remove a search result from its non-European versions. The Court of Justice answered this question in the negative. However, a search engine can be obligated to take measures that effectively prevent or seriously discourage internet users within the European Union from accessing the delisted website trough a non-European version.

In this article, I answer the following research question: 'To what extent does the right to be forgotten after Google v CNIL adequately prevent users from accessing a website from within the European Union?' The answer to this question requires a clear understanding of the right to be forgotten and the territorial scope of the GDPR. This article therefore starts with a brief description of the right to be forgotten (the section 'The Right to be Forgotten and Search Engines') and the territorial scope of the GDPR (the section 'The Territorial Scope of the GDPR'). Next, I will analyse the territorial scope of the right to be forgotten. This issue was first addressed in *Google Spain* (the section *'Google Spain'*), in which the Court of Justice ruled that data protection law and the right to be forgotten apply to (international) search engines on the basis of the establishment criterion. This ruling concerns the Data Protection Directive. It therefore does not discuss the targeting criterion of the GDPR. However, the extensive interpretation of the Court of Justice suggests that data protection law could also apply on the basis of the targeting criterion of the GDPR (the section 'The Right to be Forgotten and the Targeting Criterion'). Whereas *Google Spain* shows that data protection law applies to search engines, *Google v CNIL* also clarifies the territorial effect of the right to be forgotten itself (the section '*Google v CNIL*'). The Court of Justice ruled that a search engine is not obligated to remove a search result from its non-European versions, but that it can have an obligation to take measures to prevent European users from accessing the delisted website through the search engine. In practice, these measures primarily consist of geo-blocking. However, the section 'The effectiveness of geo-blocking' shows that geo-blocking by itself is not sufficiently effective to adequately prevent users from accessing the delisted website from within the European Union. The section 'Additional measures' discusses some of the additional measures that can be taken. Next, I will address the question whether a 'global' right to be forgotten can also be

3 Case C-131/12 *Google Spain* [2014] ECLI:EU:C:2014:317; Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ('GDPR') [2016] OJ L119/1.

4 For a discussion about other aspects of the effectiveness of this right, see eg TFE Tjong Tjin Tai, 'The Right to be Forgotten – Private Law Enforcement' (2016) 30 International Review of Law, Computers & Technology 76. See also the limitations of the right, discussed in the section 'The Right to be Forgotten and Search Engines'.

5 This issue is not restricted to search engines. Other websites such as weblogs are also offered in different versions. For example, see Hof 's-Hertogenbosch 6 October 2015, ECLI:NL:GHSHE:2015:3904 about the question whether a Dutch court can obligate a weblog to remove content from all versions.

6 Case C-507/17 *Google v CNIL* [2019] ECLI:EU:C:2019:772.

Downloaded from https://academic.oup.com/jiplt/article/29/1/57/6118444 by guest on 16 April 2021

based on national law (the section 'National Standards of Protection of Fundamental Rights'). In this light, I will also compare *Google v CNIL* with *Glawischnig-Piesczek v Facebook* (the section *'Glawischnig-Piesczek v Facebook'*). Although these cases concern different European rules, both give a large measure of discretionary power to the member. They therefore provide insight in the way European law and the Court of Justice deal with the problems that arise from the global nature of the internet. I end with a conclusion (the section 'Conclusion'). At first sight, *Google v CNIL* seriously undermines the effectiveness of the right to be forgotten.[7] However, a more thorough analysis shows that the judgement does not necessarily lead to this result.

This article analyses the right to be forgotten under the GDPR. In contrast, the requests for preliminary rulings in *Google Spain* and *Google v CNIL* concern the predecessor of the GDPR, the 'Data Protection Directive'.[8] However, the Data Protection Directive and GDPR approach the right to be forgotten in a similar way.[9] Moreover, the European Court of Justice also examines the questions in *Google v CNIL* in the light of the GDPR.[10] For these reasons, *Google Spain* and *Google v CNIL* remain relevant under the GDPR. I will therefore only pay limited attention to the Data Protection Directive.

THE RIGHT TO BE FORGOTTEN AND SEARCH ENGINES

On 2 December 2019, the European Data Protection Board (the 'EDPB') published guidelines on the criteria of the right to be forgotten in search engine cases. These guidelines are provisional. The public was able to submit comments until 5 February 2020. The EDPB has only published 'part 1' of the guidelines. This part deals with the grounds for the exercise of the right to be forgotten and the exceptions to this right. It does not address *Google v CNIL* or the territorial effect.[11]

Articles 17 and 21 GDPR provide the legal basis for the right to be forgotten.[12] In *Google Spain*, the Court of Justice ruled that the 'data subject' can use this right to

7 eg Leo Kelion, 'Google Wins Landmark Right to be Forgotten Case' (*BBC*, 24 September 2019) <www.bbc.com/news/technology-49808208> (accessed 6 May 2020); Enrique Dans, 'It's Time To Forget The Right To Be Forgotten' (*Forbes*, 25 September 2019) <www.forbes.com/sites/enriquedans/2019/09/25/its-time-to-forget-the-right-to-be-forgotten> (accessed 6 May 2020); Phil Muncaster, 'Experts Question ECJ's Right to be Forgotten Ruling' (*Infosecurity Magazine* 25 September 2019) <www.infosecurity-magazine.com/news/experts-question-ecjs-right-to-be/> (accessed 6 May 2020); Nicole Lindsey, 'EU Court Rules Google Does Not Have to Apply 'Right to Be Forgotten' Globally' (*CPOMagazine* 7 October 2019) <www.cpomagazine.com/data-privacy/eu-court-rules-google-does-not-have-to-apply-right-to-be-forgotten-globally/> (accessed 6 May 2020).

8 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31; GDPR, art 94.

9 PTJ Wolters, 'The Control by and Rights of the Data Subject Under the GDPR' (2018) 22 Journal of Internet Law 1, 9; n 10.

10 Case C-507/17 *Google v CNIL* [2019] ECLI:EU:C:2019:772, para 41. See also Case C-136/17 *GC and others* [2019] ECLI:EU:C:2019:773, para 33, where the Court of Justice takes the GDPR into account in the analysis of the questions.

11 European Data Protection Board, *Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR (part 1)* (Version for public consultation, 2019). About the EDPB, see also GDPR, art 68. For the (general) guidelines about the territorial scope, see n 23.

12 Case C-136/17 *GC and others* [2019] ECLI:EU:C:2019:773, para 65; European Data Protection Board (n 11) 3–4.

Downloaded from https://academic.oup.com/jiplp/article/29/1/57/6118444 by guest on 16 April 2021

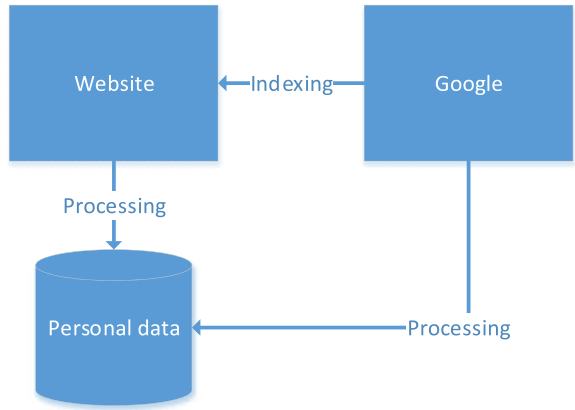

Figure 1. Google Spain

compel a search engine to remove a website from the list of search results. This judgement can be understood as follows. A website of a third party may contain 'personal data'. A search engine that indexes this website, temporarily stores it and makes it available to internet users in a particular order 'processes' these personal data and determines the purposes and means of this processing. It is therefore a 'controller'.[13] Figure 1 provides an overview of this judgement.

The processing by Google may be permitted under Article 6(1)(f) GDPR on the basis of a 'legitimate interest'. This interest is not limited to the economic interests of Google. It primarily consists of the right to freedom of information of internet users.[14] However, the data subject has the right to object to this processing on grounds relating to his or her particular situation. If this objection is successful, the search engine must remove the website from the list of search results that is displayed when a user enters, as a general rule,[15] the data subject's name as a search criterion.[16]

The right to be forgotten has several important limitations. First, the delisting does not remove the personal data from the website of the third party.[17]

13 Case C-131/12 *Google Spain* [2014] ECLI:EU:C:2014:317, paras 40–41. See GDPR, art 4(1), (2), (7) for the definitions of the concepts used in this paragraph.

14 Case C-131/12 *Google Spain* [2014] ECLI:EU:C:2014:317, paras 73, 80. The Court of Justice does not explicitly declare that these interests justify the processing by the search engine. However, the ruling that Google is obligated to delist a website *after* receiving an objection on grounds relating to the *particular* situation of the data subject suggests that the processing is generally allowed as long as the right to be forgotten has not been exercised.

15 The EDPB states that the website should be delisted for queries that include 'as a main rule', 'as a general rule' or 'in principle' the data subject's name and that the right to be forgotten is 'mainly based' on this name. European Data Protection Board (n 11) 4, 6. It thus implies that the right to be forgotten could also be extended to other search queries if this is necessary to ensure effective protection against the 'significant' and 'additional' activity of a search engine. cf Case C-131/12 *Google Spain* [2014] ECLI:EU:C:2014:317, para 38.

16 GDPR, arts 17(1)(c), 21(1); Case C-131/12 *Google Spain* [2014] ECLI:EU:C:2014:317, paras 75, 76. See also Case C-136/17 *GC and others* [2019] ECLI:EU:C:2019:773, paras 64–65. About the right to object, see GDPR, art 21(1); Wolters (n 9) 11–12.

17 Case C-131/12 *Google Spain* [2014] ECLI:EU:C:2014:317, para 88.

Downloaded from https://academic.oup.com/jiplt/article/29/1/57/6118444 by guest on 16 April 2021

Furthermore, the website is not removed from the index and cache of the search engine. The website can therefore still be found by entering a different search criterion. A data subject could also invoke Article 17 GDPR to have his or her personal data removed from the index and cache. This more extensive right exists in situations that deviate from the typical applications of the right to be forgotten.[18] It is not further discussed in this article. Finally, the exercise of the right to be forgotten does not ensure that a website is removed by all search engines. A data subject must exercise his or her right against each search engine separately.[19]

The success of the exercise of the right to be forgotten depends on the balance between the internet users' right to freedom of information and the data subject's rights to respect for private life and the protection of personal data.[20] As a general rule, the data subject's fundamental rights take precedence. However, internet users' right to freedom of information may outweigh these fundamental rights in specific cases, in particular on the basis of the role of the data subject in public life.[21]

If the website contains special categories of personal data referred to in Article 9 GDPR, the search engine can only refuse the request for delisting if the inclusion of the website is *strictly necessary* for the protection of the freedom of information. The processing of these special categories of personal data is only permitted if there is a 'substantial public interest'.[22]

THE TERRITORIAL SCOPE OF THE GDPR

Article 3 GDPR provides the territorial scope of the GDPR. The EDPB has clarified and interpreted this provision in the guidelines published on 12 November 2019.[23]

First, the GDPR may apply on the basis of the *location of the controller or processor*. Article 3(1) GDPR provides the 'establishment criterion'. The GDPR applies if the controller or processor processes personal data in the context of the activities of an establishment in the European Union. An 'establishment' exists if there is an effective and real exercise of activities through stable arrangements. This threshold is low. Even minimal activities by a single employee may be sufficient.[24] However, the mere availability of the controller's website is not.[25]

The GDPR only applies if the processing takes place in the context of the activities of this establishment. This requirement must not be interpreted restrictively.

18 European Data Protection Board (n 11) 4.

19 cf GDPR, art 19. A controller must communicate any delisting to recipients to whom the personal data have been disclosed. However, such an obligation does not exist in relation to competing search engines that perform separate indexing activities.

20 As protected by Charter of Fundamental Rights of the European Union [2012] OJ C326/391, arts 7, 8.

21 GDPR, art 17(3)(a); Case C-131/12 *Google Spain* [2014] ECLI:EU:C:2014:317, paras 69, 81; Case C-136/17 *GC and others* [2019] ECLI:EU:C:2019:773, paras 53, 66, 69; European Data Protection Board (n 11) 7–8, 10–11.

22 GDPR, art 9(2)(g); Case C-136/17 *GC and others* [2019] ECLI:EU:C:2019:773, para 61, 68–69, 75.

23 European Data Protection Board, *Guidelines 3/2018 on the territorial scope of the GDPR (Article 3). Version 2.0* (Version after public consultation, 2019). For a discussion of the territorial scope, see also De Hert and Czerniawski (n 2).

24 GDPR, recital 22; Case C-230/14 *Weltimmo* [2015] ECLI:EU:C:2015:639; European Data Protection Board, ibid 6.

25 Case C-191/15 *Verein für Konsumenteninformation* [2016] ECLI:EU:C:2016:612, para 76; European Data Protection Board (n 23) 7.

Downloaded from https://academic.oup.com/ijlit/article/29/1/57/6118444 by guest on 16 April 2021

The GDPR is intended to ensure effective and complete protection. It should not be possible to circumvent the applicability of data protection law.[26] It is therefore not required that the actual processing takes place in the European Union. The GDPR also applies if the processing in the context of the European establishment is done by an office or processor outside of the European Union.[27]

Article 3(3) GDPR extends the establishment criterion. The GDPR also applies to a controller, but not a processer, that is established in a place where member state law applies by virtue of public international law. For example, it also applies to a consulate of a member state or a ship in international waters that is registered in the European Union.[28]

The GDPR may also apply on the basis of the *location of the data subjects*. Article 3(2) GDPR provides the 'targeting criterion'. The GDPR applies to the processing of personal data of data subjects who are located within the European Union,[29] even if the controller or processor does not have a European establishment.[30] However, this criterion only applies if the processing is related to the activities referred to in subparagraphs (a) and (b).

Pursuant to Article 3(2)(a), the GDPR applies if the processing is related to the offering of goods or services to data subjects within the European Union. A payment by the data subject is not necessary. 'Information society services' with a different revenue model may therefore also fall under this criterion.[31] The controller or processor must have the intention to offer goods or services to data subjects within the European Union. This intention may become apparent through circumstances such as the fact that goods can be delivered in the European Union, the option to pay in Euros or advertisements that are aimed at European data subjects. The mere availability of a website is again insufficient.[32]

Pursuant to Article 3(2)(b), the GDPR also applies if the processing is related to the monitoring of behaviour within the European Union. This includes 'profiling' by tracking a data subject on the internet.[33] However, the GDPR does not cover an incidental processing without an objective to monitor.[34]

In contrast to the establishment criterion, the targeting criterion was not included in the Data Protection Directive. It is therefore not discussed in *Google Spain* and *Google v CNIL*. Instead, Article 4(1)(c) of the Data Protection Directive states that

26 Case C-230/14 *Weltimmo* [2015] ECLI:EU:C:2015:639, paras 25, 30; European Data Protection Board (n 23) 7–9; De Hert and Czerniawski (n 2) 234–35; n 44.

27 See also European Data Protection Board (n 23) 9–11.

28 ibid 22–23.

29 They do not have to be European citizens. GDPR, recital 14; European Data Protection Board (n 23) 14–15.

30 European Data Protection Board (n 23) 13.

31 Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (codification) [2015] OJ L241/1, art 1(1)(b); European Data Protection Board (n 23) 16. The supplier of the service may earn income by displaying personalised advertisements, which could trigger GDPR, art 3(2)(b). n 33.

32 GDPR, recital 23; European Data Protection Board (n 23) 17–18.

33 GDPR, recital 24; European Data Protection Board (n 23) 15, 19.

34 European Data Protection Board (n 23) 20.

Downloaded from https://academic.oup.com/jiplt/article/29/1/57/6118444 by guest on 16 April 2021

the Directive can also apply on the basis of the *location of the equipment* that is used to process the personal data. This criterion is not included in the GDPR.[35]

GOOGLE SPAIN

Google has a subsidiary in Spain, 'Google Spain'. This subsidiary is mainly concerned with the sale of advertising space to companies in Spain. It does not perform activities that are directly related to the indexing, storing and making available of third-party websites.[36] It therefore does not carry out any processing that is affected by the right to be forgotten.

However, the establishment criterion does not require that the processing is actually performed 'by' the establishment in the European Union. The GDPR also applies if the processing is performed in the extensively interpreted context of the activities of this establishment (the section 'The Territorial Scope of the GDPR'). The Court of Justice therefore rules that the processing of personal data for the search engine service and the sale of advertising space by the Spanish subsidiary are inextricably linked. The sale of advertising space makes the search engine economically profitable. At the same time, there would not be any advertising space to sell without the search engine. After all, the display of search results is accompanied, on the same page, by the display of advertisements.[37]

THE RIGHT TO BE FORGOTTEN AND THE TARGETING CRITERION

The preliminary ruling in *Google Spain* concerns the Data Protection Directive. The targeting criterion of the GDPR is therefore not discussed (the section 'The Territorial Scope of the GDPR'). However, the extensive interpretation of the Court of Justice suggests that, in the absence of an establishment in Spain, data protection law could also apply on the basis of the targeting criterion of the GDPR.

Google has the intention to offer its search engine service to data subjects in the European Union.[38] This service requires the indexing, storing and making available of third-party websites. Moreover, the inclusion of websites with information about European data subjects is important to ensure that the search engine also leads to relevant results for European users. For this reason, offering the search engine service and processing personal data are inextricably linked. In his conclusion in *Google Spain*, Advocate General Jääskinen therefore seems to assume that data protection law would also apply to the search engine under the targeting criterion of the proposal for the GDPR and that this result would be consistent with other European provisions.[39]

35 For a comparison between the Data Protection Directive and the GDPR, see also European Data Protection Board (n 23) 4, 6, 23; De Hert and Czerniawski (n 2); Merlin Gömann, 'The New Territorial Scope of EU Data Protection Law: Deconstructing a Revolutionary Achievement' (2017) 54 CMLR 567.

36 Case C-131/12 *Google Spain* [2014] ECLI:EU:C:2014:317, paras 43, 46, 51.

37 Case C-131/12 *Google Spain* [2014] ECLI:EU:C:2014:317, paras 52–58. See also Case C-507/17 *Google v CNIL* [2019] ECLI:EU:C:2019:772, paras 49–52.

38 This is evident from the European versions of the search engine. The sections 'Introduction', '*Google v Cnil*'.

39 Case C-131/12 *Google Spain* [2014] ECLI:EU:C:2014:317, Opinion of AG Jääskinen [2013] ECLI:EU:C:2013:424, para 56.

Downloaded from https://academic.oup.com/jiplt/article/29/1/57/6118444 by guest on 16 April 2021

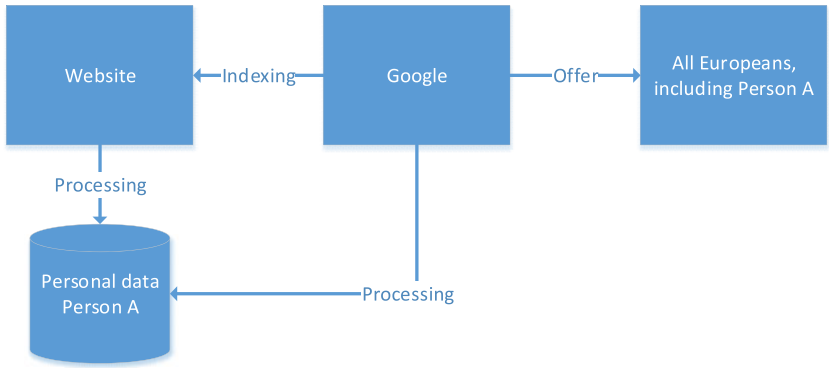

Figure 2. Targeting criterion and the right to be forgotten

A restrictive textual interpretation of Article 3(2)(a) of the GDPR would lead to a different result. The English version is rather vague. It states that the GDPR applies if the processing of personal data of European data subjects is related to the offering of goods or services *to* 'such' data subjects. Other versions more clearly point to a restrictive approach. For example, the French and Dutch versions state that the GDPR applies if the services are offered to '*ces*' or '*deze*' (= these) data subjects. These formulations suggest that the GDPR only applies if the processed personal data relate to the data subject to whom the service is offered. This is only indirectly the case with personal data on a third-party website. The search engine is available to all Europeans. The fact that it is also offered to the data subject is merely an unintended and incidental consequence. It is therefore insufficient to trigger the targeting criterion.[40] Figure 2 provides an overview of this situation.

In contrast, the German version only requires that the services are offered to '*betroffenen Personen*' (= data subjects). However, even this version shows that the GDPR at least *assumes* that the person to whom the service is offered is the data subject whose data are processed. After all, he or she would not be a data subject otherwise.

The guidelines by the EDPB do not provide clarity. The EDPB sets forth that the GDPR applies if the personal data of European data subjects is processed 'and' the service is offered in the European Union. It does not explicitly link these requirements.[41] It declares that the product must be offered to 'individuals' or a

40 cf European Data Protection Board (n 23) 15, 18, 20.

41 European Data Protection Board (n 23) 14. cf art 29 Data Protection Working Party, *Opinion 8/2010 on applicable law* (0836-02/10/EN WP 179, 2010) 31; art 29 Data Protection Working Party, *Update of Opinion 8/2010 on applicable law in light of the CJEU judgement in Google Spain* (176/16/EN WP 179 update, 2015) 2. The art 29 Data Protection Working Party states that data protection law should also apply to a processing *in the context of* services that are explicitly offered to individuals within the European Union and that *Google Spain* does not exclude the application of data protection law to a controller without an establishment in the European Union. More recent opinions about the revision of data protection law do not provide more clarity. art 29 Data Protection Working Party, *Opinion 01/2012 on the data protection reform proposals* (00530/12/EN WP 191, 2012); art 29 Data Protection Working Party, *Opinion 08/2012 providing further input on the data protection reform discussions* (01574/12/EN WP 199, 2012).

Downloaded from https://academic.oup.com/jiplp/article/29/1/57/6118444 by guest on 16 April 2021

'person' in the European Union, but also that the offer should be directed at a 'data subject'.[42]

A restrictive textual interpretation of Article 3(2)(a) of the GDPR would lead to the conclusion that the targeting criterion is not fulfilled. This would run counter to the objectives of the GDPR. It enables a search engine to avoid the application of the right to be forgotten by closing its European establishments.[43] The decision in *Google Spain* was partly based on the objective of ensuring effective and complete protection.[44] This objective could outweigh the fact that the GDPR *assumes* or *suggests* that the person to whom the service is offered is also the data subject whose data are processed. The choice for a restrictive textual interpretation is therefore not self-evident.

GOOGLE V CNIL

Google Spain shows that data protection law applies to search engines. However, it does not clarify the territorial effect of the right to be forgotten. After all, the activities of Google are not limited to the European Union. It also offers its services to users in other parts of the world. *Google Spain* does not answer the question whether European law also compels Google to adjust the search results outside of the European Union.

In *Google v CNIL*, this issue is focused on the different versions of the search engine. The French supervisory authority,[45] the 'Commission nationale de l'informatique et des libertés' ('CNIL'), ordered Google to delist websites from all versions of its search engine pursuant to the right to be forgotten. However, Google was only willing to delist websites in the versions with European domain name extensions.[46] Furthermore, it started to apply 'geo-blocking' to automatically redirect a European user to the national version that corresponds to his or her location (the section 'The Effectiveness of Geo-blocking').

The Conseil d'État assesses, and the Court of Justice presumes, that data protection law also applies to the non-European versions of the search engine. Although the search results are different in each version, they are derived from common databases and common indexing. Moreover, there are various connections between the different versions. The different versions of the search engine therefore carry out a single act of personal data processing that is inextricably linked to Google's French establishment.[47] Next, the Court of Justice considers that access to the delisted website by users outside of the European Union can also have immediate and substantial

42 European Data Protection Board (n 23) 15–19.

43 cf the section 'The Territorial Scope of the GDPR'; n 26. Although it is unlikely that Google will take this step, it could be a consideration for other search engines. They may decide not to open an establishment inside the European Union. The GDPR would still apply to the processing of the personal data of the users of those search engines.

44 Case C-131/12 *Google Spain* [2014] ECLI:EU:C:2014:317, paras 53–54.

45 See GDPR, arts 51–59 about the status, competence, tasks and powers of the supervisory authorities. Ultimately though, the capabilities of the supervisory authorities do not depend on the GDPR but on national law. See also PTJ Wolters, 'The Enforcement by the Data Subject under the GDPR' (2019) 22 Journal of Internet Law 1, 23.

46 Case C-507/17 *Google v CNIL* [2019] ECLI:EU:C:2019:772, paras 30–31. eg <www.google.de>; <www.google.fr>; <www.google.nl>.

47 Case C-507/17 *Google v CNIL* [2019] ECLI:EU:C:2019:772, paras 36–37, 52.

Downloaded from https://academic.oup.com/jiplt/article/29/1/57/6118444 by guest on 16 April 2021

effects on European data subjects.[48] The European Union therefore has the competence to obligate the delisting in all versions.[49]

Still, the Court of Justice rules that the GDPR does not impose this obligation.[50] This ruling is primarily based on the complications that a global right to be forgotten would entail. After all, such a right would greatly increase the extraterritorial effect of the GDPR.[51] It would not only prevent search engines from offering their services to users in the European Union (see also the sections 'The Right to be Forgotten and the Targeting Criterion' and 'The Effectiveness of Geo-blocking'), but also interfere with their operations in other parts of the world. The Court of Justice therefore emphasizes that numerous third states do not have the right to be forgotten or have a different approach to this right.[52] Moreover, data protection must be balanced against other fundamental rights. This balance is likely to vary significantly around the world.[53] The GDPR does not clearly create a global right to be forgotten and does not provide instruments and mechanisms to cooperate on such a right.[54] In principle, Google is obligated to delist the websites in all European versions. However, this may be different in situations in which the interest of the public in accessing information varies between member states.[55]

The judgement in *Google v CNIL* represents a pragmatic solution. It limits the regulation of the (global) world wide web to websites that are specifically targeted to users in the European Union. It therefore avoids undue encroachment of the 'digital sovereignty' of other countries.[56]

At the same time, *Google v CNIL* does not provide a general and comprehensive answer to the question whether and to what extent the GDPR has a global effect.

48 ibid, paras 54–57. See also Federico Fabbrini and Edoardo Celeste, 'The Right to Be Forgotten in the Digital Age: The Challenges of Data Protection Beyond Borders' (2020) 21 German Law Journal S1 55, 64.

49 Case C-507/17 *Google v CNIL* [2019] ECLI:EU:C:2019:772, para 58; Constanza Manavello and Laura Di Tecco,'The Global Implications of the CJEU's Ruling in Google 'Right to Be Forgotten' Case' (*IP Watchdog*, 16 October 2019) <www.ipwatchdog.com/2019/10/16/global-implications-cjeus-ruling-google-right-forgotten-case/> accessed 6 May 2020.

50 Case C-507/17 *Google v CNIL* [2019] ECLI:EU:C:2019:772, para 64.

51 cf Manavello and Di Tecco (n 49) ('political grounds'). About the complications of the extraterritorial effect of the GDPR, see also Dan Jerker B Svantesson, 'Extraterritoriality and Targeting in EU Data Privacy Law: The Weak Spot Undermining the Regulation' (2015) 5 IDPL 226; Christopher Kuner, 'Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law' (2015) 5 IDPL 235; De Hert and Czerniawski (n 2) 239–42; Fabbrini and Celeste (n 48) 55–65.

52 Case C-507/17 *Google v CNIL* [2019] ECLI:EU:C:2019:772, para 59. See also para 38. Google appeals to the principles of courtesy and non-interference of public international law. See also Mary Samonte, 'Google v CNIL Case C-507/17: The Territorial Scope of the Right to be Forgotten Under EU Law' (*European law blog* 29 October 2019) <https://europeanlawblog.eu/2019/10/29/google-v-cnil-case-c-507-17-the-territorial-scope-of-the-right-to-be-forgotten-under-eu-law/> accessed 6 May 2020.

53 Case C-507/17 *Google v CNIL* [2019] ECLI:EU:C:2019:772, para 60. For comparisons with other countries, see eg Oskar J Gstrein, 'The Judgment That Will Be Forgotten' (*Verfassungsblog*, 25 September 2019) <https://verfassungsblog.de/the-judgment-that-will-be-forgotten/> accessed 6 May 2020 (noting that the right exists in many jurisdictions); Manavello and Di Tecco (n 49) (USA); Andrew K Woods, 'Three Things to Remember from Europe's "Right to Be Forgotten" Decisions' (*Lawfare* 1 October 2019) <https://www.lawfareblog.com/three-things-remember-europes-right-be-forgotten-decisions> accessed 6 May 2020 (Canada); Fabbrini and Celeste (n 48) 55.

54 Case C-507/17 *Google v CNIL* [2019] ECLI:EU:C:2019:772, paras 61–63.

55 ibid paras 66–69.

56 Fabbrini and Celeste (n 48) 64.

Downloaded from https://academic.oup.com/jiplit/article/29/1/57/6118444 by guest on 16 April 2021

Most importantly, the ultimate rejection of an obligation to delist a website in all versions is accompanied by the insistence that the European Union does have the competence to impose such an obligation. The Court of Justice does not reject any and all application of the GDPR to these non-European versions, it only rejects the global right to be forgotten.

Furthermore, the solution of *Google v CNIL* is limited to the context of international search engines with different national versions. It does not clarify whether a global right to be forgotten exists in other situations. For example, *Google v CNIL* does not address the situation in which a single version is used to target both European and international users. The insistence on the applicability of the GDPR and the competence to impose a global right to forgotten suggests that the Court of Justice may impose an obligation to delist such a situation. After all, search engines who wish to avoid this global interference can decide to offer different versions for different parts of the world. In contrast, such an obligation may not exist for search engines that do not target European users at all, especially when they do not have a European establishment (see also the section 'The Right to be Forgotten and the Targeting Criterion').

THE EFFECTIVENESS OF GEO-BLOCKING

The solution of *Google v CNIL* would not adequately protect data subjects if users could simply circumvent the application of the right to be forgotten by using a non-European version of a search engine. For this reason, the Court of Justice also decided that, 'if necessary', the search engine must take measures that are 'sufficiently effective' to ensure the effective protection of the fundamental rights of the data subject. The measures should prevent or at least seriously discourage users in the European Union from accessing the delisted website through a search with the name of the data subject as a search criterion.[57]

According to the Court of Justice, Google uses geo-blocking for this purpose. It automatically redirects a user to the national version of the search engine that corresponds to his or her location. This location is determined by the user's IP address.[58] For example, a user with a 'Dutch' IP address will be automatically redirected to 'Google.nl', even if it enters '.com' or any other domain name extension. The user therefore cannot find the delisted website through a search with the name of the data subject as a search criterion. Figure 3 provides an overview of this solution.

The ruling of the Court of Justice is 'technology neutral'. It prescribes 'sufficiently effective measures', but not that these measures should consist of geo-blocking on the basis of the user's IP address. Moreover, it does not address the question whether the measures of Google are sufficiently effective. This is for the referring court to ascertain.[59]

57 Case C-507/17 *Google v CNIL* [2019] ECLI:EU:C:2019:772, para 70.

58 ibid, paras 32, 42–43.

59 ibid, para 71; Manavello and Di Tecco (n 49). In the conflict between Google and CNIL, the Conseil d'État did not address this issue. Instead, it decided that CNIL lacked the power to order a global delisting. Conseil d'État 27 March 2020, No 399922; the section 'National Standards of Protection of Fundamental Rights'.

Downloaded from https://academic.oup.com/jiplp/article/29/1/57/6118444 by guest on 16 April 2021

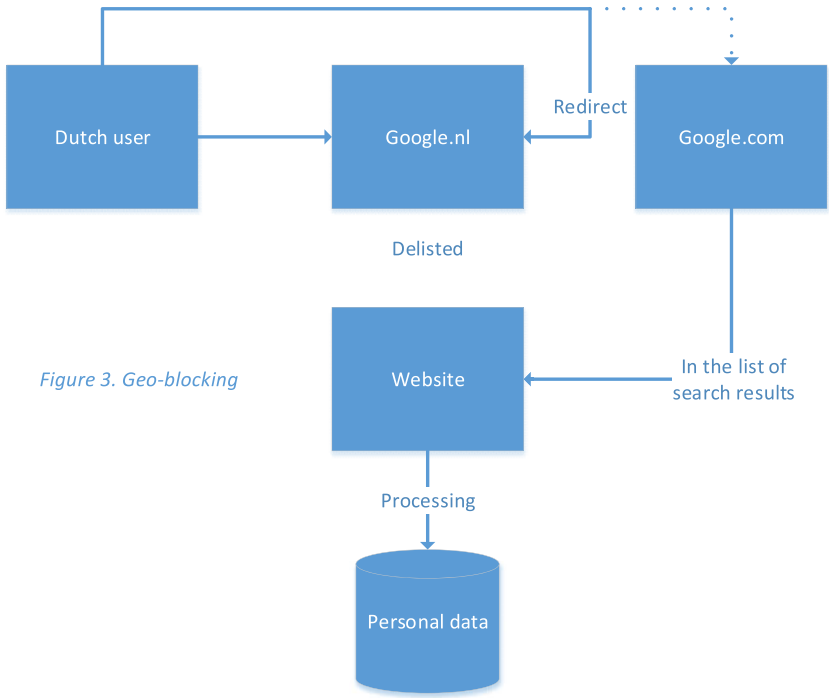

Figure 3. Geo-blocking

Figure 3. Geo-blocking

The effectiveness of geo-blocking depends on several factors. First, accuracy is important. Geo-blocking will not provide effective protection if Google mistakenly determines that certain IP addresses belong to locations outside of the European Union. This risk appears to be limited. Although geo-blocking is not always precise, the country of the user is usually determined correctly.[60] The location can be determined more precisely by using available Wi-Fi networks, GPS or the mobile phone network.[61] However, these techniques require the users to share their location with Google. This is not necessary if the location is determined by using the IP address.

60 eg Ingmar Poese and others, 'IP Geolocation Databases: Unreliable?' (2011) 41 ACM SIGCOMM Computer Communication Review 53; Manaf Gharaibeh and others, 'A Look at Router Geolocation in Public and Commercial Databases' in *IMC'17 Proceedings of the 2017 Internet Measurement Conference* (ACM 2017). The determination of the location could temporarily become less accurate due to the switch from IPv4 to IPv6. Jan-Jelle Kester, 'Comparing the Accuracy of IPv4 and IPv6 Geolocation Databases' (*JJKester*, 22 January 2016) <www.jjkester.nl/projects/geoip/> accessed 6 May 2020; Scott Hogg, 'Determining where you are using IPv6' (*Infoblox*, 7 November 2017) <https://blogs.infoblox.com/ipv6-coe/geolocation-with-ipv6/> accessed 6 May 2020; Jason Young, 'Geolocation and Mobile Data' (*Mobile Reading Data Exchange* 6 March 2018) <https://tascha.github.io/Mobile-Reading-Data-Exchange/2018/03/06/geolocation-and-mobile-data.html> accessed 6 May 2020.

61 eg art 29 Data Protection Working Party, *Opinion 13/2011 on Geolocation services on smart mobile devices* (881/11/EN WP 185, 2011) 4–5; Anthony T Holdener III, *HTML5 Geolocation* (O'Reilly 2011) 7–12; Anna Sainsbury, 'Geolocation Basics' (2013) 17 Gaming Law Review and Economics 33, 34–35. The location can also be determined through profiling. eg if a user regularly searches for restaurants in New York and creates a profile that lists 'New York' as the home address, Google could assume that he or she

Downloaded from https://academic.oup.com/jiplp/article/29/1/57/6118444 by guest on 16 April 2021

Next, the effectiveness depends on the possibilities to circumvent geo-blocking. For example, this can be done by using a 'proxy server', 'virtual private network' ('VPN') or the 'Tor' web browser.[62] These tools all function in a similar way.[63] They mask the IP address, and thus the location, of the user by routing internet traffic through a non-European server. This causes Google to mistakenly determine that a user is located outside of the European Union and thus include the delisted website in the search results. These 'circumvention tools' are relatively easy to use, at least in the European Union.[64] They are also quite popular. About a quarter of the internet users occasionally use a VPN.[65] The chance that a European user accesses a delisted website through a search engine is therefore not negligible.

This is especially important because the right to be forgotten only applies to *targeted* searches. The right only obligates the search engine to delist the website when the name of the data subject is used as a search criterion (the section 'The Right to be Forgotten and Search Engines'). In this scenario, a user made a conscious effort to specifically search for information about the data subject. Performing such a search with a VPN only requires limited additional effort. Moreover, the right to be forgotten is quite popular. Since *Google Spain*, Google has delisted over 1.4 million URLs.[66] A user of a search engine can therefore know that there is a small but not negligible chance that his 'target' has also used the right to be forgotten. For example, recruiters could decide to always use a VPN when using the name of an applicant as a search criterion. The effectiveness of geo-blocking is therefore limited. The effectiveness of the right to be forgotten falters in the scenarios where the data subject needs it most.

Geo-blocking is therefore not 'sufficiently effective' and does ensure the 'effective protection' of the data subject. The referring court should conclude that Google violates the right to be forgotten. The easiest way to remedy this violation is to delist the website in all versions of the search engine. Through this 'detour', the right to be forgotten may still have global effect.

is located outside of the European Union. However, this method is no longer accurate if the user subsequently goes on a vacation in Rome. For another example, see Massimo La Morgia and others, 'Nationality and Geolocation-Based Profiling in the Dark(Web)' IEEE Transactions on Services Computing (online access) (using the time of activity and the language of the user to determine his or her location).

62 See also n 7.

63 For a general description, see Hal Roberts and others, *2010 Circumvention Tool Usage Report* (The Berkman Center for Internet & Society 2010); Kirk A Duncan, *Assessing the use of Social Media in a Revolutionary Environment* (Naval Postgraduate School 2013) 36–37. About Tor, see La Morgia and others (n 61) 2.

64 The risks and barriers are larger in countries with more internet censorship. Duncan (n 63) 37–38. Even so, the circumvention tools are especially popular in those countries. Yi Mou, Kevin Wu and David Atkin, 'Understanding the use of Circumvention Tools to Bypass Online Censorship' (2016) 18 New Media & Society 837; n 65.

65 Oliva Valentine, 'VPN Usage Across the World' (*Globalwebindex*, 2 July 2018) <https://blog.globalwebindex.com/chart-of-the-day/vpn-usage-2018/> accessed 6 May 2020; J Clement, 'Global VPN Usage Reach 2018, by Region' (*statista*, 22 July 2019) <www.statista.com/statistics/306955/vpn-proxy-server-use-worldwide-by-region/> accessed 6 May 2020. Only 3% used a VPN or other circumvention tool in 2010. Roberts and others (n 63) 3.

66 <https://transparencyreport.google.com/eu-privacy/> (1.450.380,accessed 6 May 2020).

Downloaded from https://academic.oup.com/jiplit/article/29/1/57/6118444 by guest on 16 April 2021

ADDITIONAL MEASURES

Alternatively, Google could remedy a violation of the right to be forgotten by taking additional measures. For example, the search engine could also 'filter' the delisted websites from the search results when a user employs a VPN or other circumvention tool. This solution works on another level than the currently used geo-blocking. Instead of blocking access to other versions of the search engine, it blocks access to individual search results. Such a solution could also be used by search engines and other websites that do not have different national versions (see the section '*Google v CNIL*'). Google could even choose to completely block the use of its search engine by users that employ a circumvention tool.

These solutions have important disadvantages. First, Google must be able to reliably discover and block the circumvention tools. This can be done by using various techniques that are also used by companies such as Netflix and other streaming services.[67] However, they are not perfect.[68] Ensuring their effectiveness would require continuous investments. Nevertheless, there is no obligation to guarantee that the measures work perfectly. *Google v CNIL* only requires that the measures are 'sufficiently effective'.

Next, these solutions can restrict the right to freedom of information, especially when access to the search engine is completely blocked. Users in China and other countries with more severe internet censorship need the circumvention tools to access an uncensored search engine.[69] The impact of filtered search results is more limited. Google could pair the filter with a message that some search results may have been removed in accordance with the right to be forgotten.[70] Under this solution, a user outside of the European Union could find the delisted websites by searching again without the circumvention tool.

This solution becomes more problematic if it is also applied to meet delisting obligations of other countries. The European right to be forgotten primarily applies to information that may be considered sensitive by an individual data subject but is relatively unimportant for the society as a whole. In contrast, other countries may

67 eg Lucas Dixon, Thomas Ristenpart and Thomas Shrimpton, 'Network Traffic Obfuscation and Automated Internet Censorship' (2016) 14 IEEE Security & Privacy 43, 44–49; Jon Watson, 'How Easy is it to Detect a VPN is being Used?' (*comparitech.com* 29 November 2017) <www.comparitech.com/blog/vpn-privacy/how-easy-is-it-to-detect-a-vpn/> accessed 6 May 2020; Darragh Delaney, 'How to Passively Detect VPN Clients on Your Network' (*Netfort* 5 December 2017) <www.netfort.com/blog/detect-vpn-clients-network/> accessed 6 May 2020; n 69.

68 eg Paul Bischoff, 'Best VPNs for Netflix: Get any version of Netflix anywhere' (*comparitech* 2 March 2020) <www.comparitech.com/blog/vpn-privacy/netflix-vpn-unblock-proxy-error/> accessed 6 May 2020; n 69.

69 Daniel Anderson, 'Splinternet Behind the Great Firewall of China' (2012) 10[11] ACM Queue.

70 Google displays a similar message if results are deleted pursuant to the 'US Digital Milennium Copyright Act'. eg the search criterion 'watch the avengers online' (6 May 2020, my personal laptop, Firefox with private browsing) was paired with the message 'In response to multiple complaints that we received under the US Digital Millennium Copyright Act, we have removed 7 results from this page. . . . '. A comparable message was shown outside of the context of IP law with the censored Chinese version of Google. Elliot D Cohen, *Mass Surveillance and State Control. The Total Information Awareness Project* (Palgrave Macmillan 2010) 81.

Downloaded from https://academic.oup.com/jiplp/article/29/1/57/6118444 by guest on 16 April 2021

impose obligations to remove politically sensitive or otherwise important information.[71] The solution could thus expose the users of circumvention tools to the censorship of various countries. This also affects users in Europe and other counties with a relatively high level of internet freedom. It will be more difficult for them to exercise the right to freedom of information while retaining the (real or hypothetical) 'right to anonymity'.[72]

NATIONAL STANDARDS OF PROTECTION OF FUNDAMENTAL RIGHTS

In *Google v CNIL*, the Court of Justice rules that the GDPR does not *create* a global right to be forgotten. However, neither does European law *prohibit* such a right. The Court of Justice explicitly declares that national standards of protection of fundamental rights could still obligate a search engine to also delist a website in its non-European versions.[73] In the conflict between Google and CNIL, the Conseil d'État has since decided that CNIL cannot order a global delisting in the absence of national legislation that grants this power. Furthermore, it stated that such an order would require balancing the rights to data protection and freedom of information on a case-by-case basis.[74]

The decision that European law does not prohibit a 'national' global right to be forgotten raises several issues about the relationship between national and European law. First, the objectives of the GDPR include the harmonization of data protection law, the creation of a consistent level of protection and ensuring the free movement of personal data.[75] A national global right to be forgotten would undermine these

71 See also Fabbrini and Celeste (n 48) 64–65.

72 Note that this 'right' or principle is not discussed in *Google v CNIL*. About this right, see eg Council of Europe, Committee of Ministers, *Declaration on freedom of communication on the Internet* (28 May 2003), principle 7; Jonathan Turley, 'Registering Publius: The Supreme Court and the Right to Anonymity' in Roger Pilon and others (eds), *Cato Supreme Court Review* (Cato Institute 2002) 77–82; C Nicoll, JEJ Prins and MJM van Dellen (eds), *Digital Anonymity and the Law: Tensions and Dimensions* (T.M.C. Asser Press 2003); Paul de Hert, Bert-Jaap Koops and Ronald Leenes, '8. Conclusion' in Bert-Jaap Koops, Ronald Leenes and Paul de Hert (eds), *Constitutional Rights and New Technologies* (Tilburg Institute for Law, Technology, and Society 2007) 160; art 19, *Right to Online Anonymity* (2015). Retaining anonymity is not completely impossible. For example, a user could use a tool that hides his or her identity without masking the country of origin. cf <www.startpage.com>. This search engine uses the search results of Google, but does not process the personal data of its users. It only uses a country code, based on the IP address, to adapt the search results to the country of the user. <https://support.startpage.com/index.php?/Knowledgebase/Article/View/768/0/how-do-you-know-my-language-or-location-if-you-dont-store-information-about-me> accessed 6 May 2020. This solution is not completely anonymous. Startpage can still see the IP address of the user. Furthermore, this solution requires that Google trusts the country code generated by Startpage. This is only possible if Startpage takes adequate measures against the use of a VPN and other circumvention tools.

73 Case C-507/17 *Google v CNIL* [2019] ECLI:EU:C:2019:772, para 72; Woods (n 53).

74 Conseil d'État 27 March 2020, no 399922.

75 GDPR, art 1, recitals 2, 3, 6, 7, 9, 10, 11, 13, 53, 123, 166, 170; Viviane Reding, 'The European Data Protection Framework for the Twenty-first Century' (2012) 2 IDPL 119, 121; Bart van der Sloot, 'Do Data Protection Rules Protect the Individual and Should They? An Assessment of the Proposed General Data Protection Regulation' (2014) 4 IDPL 307, 317; Paul de Hert and Vagelis Papakonstantinou, 'The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?' (2016) 32 Computer Law & Security Review 179, 182; PTJ Wolters, 'The Security of Personal Data under the GDPR: A Harmonized Duty or a Shared Responsibility?' (2017) 7 IDPL 165, 165.

Downloaded from https://academic.oup.com/jiplt/article/29/1/57/6118444 by guest on 16 April 2021

objectives.[76] It would create differences in the level of protection between various member states. By ruling that the GDPR does not prohibit such a national right, the Court of Justice accepts that such differences could come into existence. Apparently, the freedom to apply national standards of protection of fundamental rights outweighs the exception to the harmonization of data protection law.[77]

Next, a global right to be forgotten leads to various complications (the section '*Google v CNIL*'). The Court of Justice does not address the question whether these complications also affect a 'national' right to be forgotten. In fact, individual member states may find them even harder to navigate. After all, the European Union has several options to ensure the extraterritorial effect of its legal rules, including its data protection law.[78]

For example, Article 44 GDPR states that transfers of personal data to third countries are only allowed under certain conditions. This allows the European Commission to make demands on the protection of personal data before it decides that a country provides an 'adequate level of protection'.[79] Furthermore, the European Union can place demands on the protection of personal data in third countries through the (approval of) codes of conduct, certification mechanisms and binding corporate rules that are used by the controller to provide 'appropriate safeguards'.[80] Among other requirements, an adequate level of protection and appropriate safeguards require that data subjects are able to enforce data protection law.[81] Furthermore, the European Commission and supervisory authorities have a duty to develop international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data.[82] Through these instruments, the European Union can enable the application of the *European* right to be forgotten in third countries. Individual member states do not have these options,

76 See also Gstrein (n 53). cf Case C-617/10 *Åkerberg Fransson* [2013] ECLI:EU:C:2013:105, para 29; Case C-399/11 *Melloni* [2013] ECLI:EU:C:2013:107, para 60. In these judgements, the Court of Justice ruled that the Charter of Fundamental Rights of the European Union does not preclude the application of national standards of protection of fundamental rights, provided that the level of protection provided for by the Charter and the primacy, unity and effectiveness of EU law are not compromised. In *Google v CNIL*, the Court of Justice refers to these judgements. See also Charter of Fundamental Rights of the European Union, art 53; Case C-469/17 *Funke Medien* [2019] ECLI:EU:C:2019:623, para 32; Case C-516/17 *Spiegel Online* [2019] ECLI:EU:C:2019:625, para 21.

77 Of course, this is not the only exception to the harmonization. See eg GDPR, arts 6(2), 8(1), 9(4); Peter Blume, 'Will it be a Better World? The Proposed EU Data Protection Regulation' (2012) 2 IDPL 130, 132–33; Simon Davies, 'The Data Protection Regulation: A Triumph of Pragmatism over Principle?' (2016) 2 EDPL 290, 294–96.

78 Kuner (n 51) 239–41; Christopher Kuner, 'The Internet and the Global Reach of EU Law' in Marise Cremona and Joanne Scott (eds), *EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law* (OUP 2019) 124–27, 130–36: Joanne Scott, 'The Global Reach of EU Law' in Marise Cremona and Joanne Scott (eds), *EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law* (OUP 2019) 21–63; Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (OUP 2020) ch 5; Fabbrini and Celeste (n 48) 64–65.

79 GDPR, art 45(1), 4. See also Kuner (n 78) 124–25.

80 GDPR, art 46. See also Kuner (n 78) 125–26.

81 See eg GDPR, arts 45(2)(a), (b), 46(1), (3)(b), 47(1)(b), (2)(e), recitals 104, 108; art 29 Data Protection Working Party, *Adequacy Referential* (18/EN WP 254 rev.01, 2018), ch 3, A8, C; art 29 Data Protection Working Party, *Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules* (18/EN WP 256 rev.01 2018) 6–7.

82 GDPR, art 50(a). See also GDPR, art 45(5), (6).

Downloaded from https://academic.oup.com/ijlit/article/29/1/57/6118444 by guest on 16 April 2021

or only to a limited extent. The enforcement of a *national* global right to be forgotten may therefore be even more problematic than the enforcement of a (hypothetical) European right.

GLAWISCHNIG-PIESCZEK V FACEBOOK

In *Glawischnig-Piesczek v Facebook*,[83] the Court of Justice arrives at a result that is similar to *Google v CNIL*. The 'e-Commerce Directive' limits the liability of certain online intermediaries.[84] Article 15 provides that the member states are not allowed to impose a general obligation to monitor on providers of 'mere conduit', 'caching' and 'hosting' services. However, the Court of Justice rules that a hosting service provider such as Facebook[85] can be ordered to remove or block information that is identical or equivalent to information that was previously declared to be unlawful.

Furthermore, the Court of Justice rules that the e-Commerce Directive does not provide for any territorial limitation on the scope of the measures that the member states are entitled to adopt. A member state is therefore allowed to order the provider of a hosting service to remove or block the information globally.[86] Although the Court of Justice states that such orders should stay within the framework of relevant international law, it does not clarify what rules are involved and to what extent these rules limit the admissibility of the order. It only refers to recitals 58 and 60 of the e-Commerce Directive.[87] These recitals do not provide clarity. They merely state in general terms that the directive is without prejudice to the results of discussions within international organizations such as WTO, OECD and UNCITRAL.

There are clear differences between the GDPR and the e-Commerce Directive. The GDPR imposes extensive obligations while the e-Commerce Directive prohibits the member states from imposing obligations.[88] Nevertheless, the result is the same.[89] European law does not impose an obligation to censor the internet globally, but it does not prohibit national law from doing so either. Moreover, the Court of Justice only provides very limited guidance about the complications that such an extensive territorial effect can entail (see also the section '*Google v CNIL*').

With the 'Digital Single Market' strategy and the priority 'A Europe fit for the digital age', the European Commission is strongly committed to a European

83 Case C-18/18 *Glawischnig-Piesczek v Facebook* [2019] ECLI:EU:C:2019:821.

84 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market [2000] OJ L178/1; n 88.

85 Case C-18/18 *Glawischnig-Piesczek v Facebook* [2019] ECLI:EU:C:2019:821, para 22.

86 ibid, paras 49–50.

87 ibid, paras 51–52; Lorna Woods, 'Facebook's Liability for Defamatory Posts: The CJEU Interprets the e-commerce Directive' (*EU Law Analysis*, 7 October 2019) <http://eulawanalysis.blogspot.com/2019/10/facebooks-liability-for-defamatory.html> accessed 6 May 2020.

88 This contrast should not be generalized. eg the e-Commerce Directive imposes duties to provide information. e-Commerce Directive, arts 5, 6, 7. The GDPR is also intended to guarantee the free movement of personal data and therefore prohibits member states from imposing additional obligations. n 75.

89 cf Fabbrini and Celeste (n 48) 62, who claim that *Glawischnig-Piesczek v Facebook* 'counter-balances' the limitation of extraterritorial effect in *Google v CNIL*. However, the apparent contrast between these judgements results from the discussed differences between the GDPR (imposing certain obligations) and e-Commerce Directive (prohibiting member states from imposing certain obligations).

Downloaded from https://academic.oup.com/jiplp/article/29/1/57/6118444 by guest on 16 April 2021

approach to digitalization.[90] At the same time, *Google v CNIL* and *Glawischnig-Piesczek v Facebook* show that European law does not yet provide a satisfactory solution to issues in relation to digitalization and extraterritoral effect.[91] In both cases, the Court of Justice refuses to give a unambiguous answer about the territorial effect of European law. Instead, it gives a large measure of discretionary power to the member states. The similarity of these cases suggests that the same result may also apply to other legal norms, other digital services[92] and (more general) other problems that arise from the global nature of the internet.

CONCLUSION

In this article, I answer the following research question: 'To what extent does the right to be forgotten after Google v CNIL adequately prevent users from accessing a website from within the European Union?' In accordance with the principles of the GDPR, the territorial effect of the right to be forgotten should not be construed too restrictively (the sections The Territorial Scope of the GDPR', *Google Spain and* 'The Right to be Forgotten and the Targeting Criterion'). In *Google v CNIL*, the Court of Justice therefore presumes that the GDPR also applies to the non-European versions of the search engine. However, the right to be forgotten does not compel the search engine to delist a website in these versions (the section '*Google v CNIL*'). At first sight, *Google v CNIL* therefore turns the right to be forgotten in a paper tiger.[93] However, further analysis reveals that this conclusion is premature.

First, much depends on the requirements on the measures to prevent or at least seriously discourage users in the European Union from accessing the delisted website. The Court of Justice does not address the question whether Google's measures are 'sufficiently effective'. This is for the referring court to ascertain. Geo-blocking can be circumvented quite easily. If the measure is nevertheless considered to be sufficiently effective, the right to be forgotten will not adequately prevent users from accessing the delisted website from within the European Union. After all, for a user who specifically searches for information about a data subject, the use of a VPN or other circumvention tool only requires limited additional effort (the section 'The Effectiveness of Geo-blocking'). However, the requirement that the measures are 'sufficiently effective' could also impose an obligation to take more effective additional measures (the section 'Additional Measures').

Furthermore, the requirements of national standards of protection of fundamental rights can also prevent users from accessing the delisted website. The GDPR does not prohibit member states from ordering search engines to also delist a website in non-European versions. Such a national enhancement of the right to be forgotten can improve the protection of the data subject but may not be easy to enforce (the

90 Commission, 'A Digital Single Market Strategy for Europe' (Communication) COM (2015) 192 final; <https://ec.europa.eu/digital-single-market/en>; <https://ec.europa.eu/info/priorities/europe-fit-digital-age_en>. Both websites accessed on 6 May 2020.

91 Gstrein (n 53); Woods (n 87). See also Kuner (n 78) 139–40, 145.

92 The dictum of *Google v CNIL* is limited to search engines. See also the section 'The Right to be Forgotten and the Targeting Criterion'. In contrast, the dictum of *Glawischnig-Piesczek v Facebook* is formulated to apply to all types of hosting services, and not just social media.

93 n 7.

Downloaded from https://academic.oup.com/jiplp/article/29/1/57/6118444 by guest on 16 April 2021

section 'National Standards of Protection of Fundamental Rights'). It remains to be seen whether and to what extent the member states will try to impose such a 'national' global right to be forgotten, especially since the Court of Justice has not provided any clear guidance about the complications of such a right. Moreover, *Glawischnig-Piesczek v Facebook* shows that this issue is not limited to the right to be forgotten. The same result also applies to other problems that arise from the global nature of the internet (the section '*Glawischnig-Piesczek v Facebook*').

The right to be forgotten is at a crossroads. *Google v CNIL* raises several questions. The answers to these questions will determine whether the right to be forgotten will adequately prevent users from accessing a website from within the European Union and provide protection in a global World Wide Web. For this reason, the effectiveness of the right to be forgotten can go either way.

Downloaded from https://academic.oup.com/jiplp/article/29/1/57/6118444 by guest on 16 April 2021